FACT Firmware Analysis

March 26, 2018

1 Meta Daten

size : 3378139

release_date : 2007-09-06

version : 1.0.4

vendor : Cisco/Linksys

hid : Cisco/Linksys SRW2008 - 1.0.4

device_class : Switch (Managed)

device_name : SRW2008

2 Analysis

2.1 base64decoder

analysis_date : 1521817964.146681

summary : []

plugin_version : 0.1.2

2.2 cpu architecture

analysis_date : 1521817974.13303

summary : []

plugin_version : 0.3.1

2.3 crypto material

analysis_date : 1521817950.2504122

summary : []

plugin_version : 0.5

2.4 exploit mitigations

analysis_date : 1521817968.7478507

summary : []

plugin_version : 0.1.1

2.5 file hashes

ssdeep : 98304:nNasK108t/KzpM7NURKVt9RMN6sc0KzLgP:nNFK1Dt/KFMX0670KIP

ripemd160 : 5e0313f309e610bece33bfece02a933bb80bc7b9

sha1 : 5ea563d79a7ed3f8c7a872e0bf31db9ef8c90711

sha512 : 937f575dfffcfe1f986faf4ca8e3ba836f6d6f9dfaab582c4561fa93c7c2b0ceee92efdb3e3e87abe0bbf9a86

sha256 : b7c55a6de9fd1b85ec07f661b4d21638021999e2b1e754de1922f3b01f2cedb8

plugin_version : 1.0

imphash : None

md5 : 9665a7ad243bda91ce6312ed3aab305d

analysis_date : 1521817977.8009713

whirlpool : 69477a040d3430dc6706d1bb6a4e2088814e24e6f3d73eb14b2e0e41aee6ba0220d98a4896b872abd558c9

2.6 file type

mime : firmware/ros

full : ROS Container

analysis_date : 1521817966.6970117

summary : [’firmware/ros’]

plugin_version : 1.0

2.7 init systems

analysis_date : 1521817971.601984

summary : []

plugin_version : 0.4.1

2.8 ip and uri finder

```
ips_v4 : [’1.0.4.1’]

uris : []

ips_v6 : [’B::’, ’3::’, ’::6B’, ’::4’, ’5::’, ’::c’, ’::D’, ’E::’, ’::9a9’, ’b::’, ’0::’, ’::’, ’A

plugin_version : 0.4.1

analysis_date : 1521817941.3742175

summary : [’1.0.4.1’, ’B::’, ’3::’, ’::6B’, ’::4’, ’5::’, ’::c’, ’::D’, ’E::’, ’::9a9’, ’b::’, ’0:
```

2.9 software components

```
analysis_date : 1521817953.0442727

summary : []

plugin_version : 0.3
```

2.10 printable strings

```
strings : [’\t\nX^|v’, ’\t\x0b?\n1F’, ’\t\x0bpNRC>’, ’\t\r1r\\V$_’, ’\t\r\\h8D’, ’\t \x0bCcn#’, ’\

analysis_date : 1521817947.8021855

plugin_version : 0.2
```

2.11 users and passwords

```
analysis_date : 1521817960.2657604

summary : []

plugin_version : 0.4
```

2.12 string evaluator

```
string_eval : [’char OGCFG_link_time[] = " 09:11:40";\r\nchar OGCFG_link_date[] = " 06-Sep-2007";\

analysis_date : 1521817957.2273827

plugin_version : 0.2
```

2.13 unpacker

```
output : ROS PACK firmware archive payload extractor
Version 0.6
(c) Copyright 2015 TJ <hacker@iam.tj>
Licensed on the terms of the GNU General Public License version 2

Filename:          /media/data/fact_fw_data/b7/b7c55a6de9fd1b85ec07f661b4d21638021999e2b1e754de192
File length:       3378139 (0x338bdb)
ARC Magic:         LSS2
ARC Index:         1.01
Header    version: 1
           length: 48
Payload
           length: 3378091 (0x338bab)
         checksum: 430634778 (0x19aaf71a)
Link Time:         09:12:58
Link Date:         2007-09-06
Signature:         PACK
Dir Entries:       6
Extracted CLI_FILE from offset 272 (105518 bytes)
Extracted DELSCRF from offset 105822 (262313 bytes)
Extracted EWS_FILE from offset 368135 (413361 bytes)
Extracted UPNP_FILE from offset 781528 (8407 bytes)
Extracted DATETIME_C from offset 789935 (160 bytes)
Extracted RSCODE from offset 790127 (2588012 bytes)

Payload      length: 3378091 (0x338bab)
Payload   extracted: 3378091 (0x338bab)
Payload    checksum: 430634778 (0x19aaf71a)
Calculated checksum: 430634778 (0x19aaf71a)
```

```
summary : ['no data lost']

plugin_version : 0.7

size packed -> unpacked : 3.22 MiB -> 3.22 MiB

plugin_used : ROSFile

number_of_unpacked_files : 6

entropy : 0.896769379976

analysis_date : 1521817932.5134149
```

2.14 malware scanner

```
scans : {'ClamAV': {'detected': False, 'version': 'ClamAV 0.99.4/24413/Fri Mar 23 13:22:23 2018\n'
```

```
scanners : ['ClamAV']

number_of_scanners : 1

plugin_version : 0.3

system_version : 0.2.6

md5 : 9665a7ad243bda91ce6312ed3aab305d

analysis_date : 1521817943.16636

summary : []

positives : 0
```